Hindawi
Science and Technology of Nuclear Installations
Volume 2020, Article ID 8839399, 9 pages
https://doi.org/10.1155/2020/8839399

Research Article

Reliability Assessment for a Safety-Related Digital Reactor Protection System Using Event-Tree/Fault-Tree (ET/FT) Method

Qingzhu Liang,[1] Mingxing Liu,[2] Peng Xiao,[2] Yun Guo,[1] Jun Xiao ,[3] and Changhong Peng[1]

[1]*School of Nuclear Science and Technology, University of Science and Technology of China, Hefei, China*
[2]*Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu, China*
[3]*Nuclear and Radiation Safety Center, Ministry of Ecology and Environment (MEE) of the People's Republic of China, Beijing, China*

Correspondence should be addressed to Jun Xiao; xiaojun70@163.com

Received 22 September 2020; Accepted 17 November 2020; Published 30 November 2020

Academic Editor: Massimo Zucchetti

Copyright © 2020 Qingzhu Liang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The aim of this study is to verify if the reliability of a digital four-channel RPS under the design phase satisfies the specified target and to identify the weakness of system design and potential solutions for system reliability improvement. The event-tree/fault-tree (ET/FT), which is the method used in the current probabilistic safety assessment (PSA) framework of nuclear power plants (NPPs), was adopted to developed reliability modeling for the RPS with the Top Events defined as the system failure to generate reactor trip signal and the system generating spurious trip signal. The evaluation results indicate that the probability of the system failure on demand and the frequency of spurious trip signal generation are 1.47×10^{-6} with a 95% upper bound of 4.63×10^{-6} and 7.94×10^{-4}/year with a 95% upper bound of 2.50×10^{-3}/year, respectively. The importance and sensitivity analyses were conducted and it was found that undetected unsafe common cause failures (CCFs) of signal conditioning modules (SCMs) dominate the system reliability. Two preliminary optimization schemes relative to reducing periodic test interval and adapting two kinds of diverse SCMs were proposed. Results of the quantitive evaluation of the schemes show that neither of them could determinedly improve the system reliability to the target level. In the future, more detailed optimization analysis shall be required to determine a feasible system design optimization scheme.

1. Introduction

The reactor protection system (RPS) is one of the most important safety-related systems in NPPs nuclear power plants (NPPs). It protects the integrity of the safety barriers of NPPs by generating signals to scram or drive engineered safety features when necessary. Obviously, the reliability of the RPS has an important impact on the plant safety and should be demonstrated to satisfy a certain level. With the rapid development of computer technology, digital technologies, which can provide potential to improve the system reliability through special features such as online self-diagnosis, are gradually adopted in the RPS [1]. It is necessary to develop reliability modeling for digital RPS and integrate the system model into probabilistic safety assessment (PSA) of NPPs.

So far there is no consensus on methods for reliability modeling of the digital system in NPPs. Even though some dynamic methods with great potential, for example, dynamic flow-graph methodology, have been proposed, they are still within the usage trial phase [2, 3]. Furthermore, the application of a dynamic method needs substantial effort and the method generally suffers from the incompatibility with the existing PSA framework. On this viewpoint, the ET/FT method that has a mature theory and is easy-to-use got much attention and had been used in research about reliability assessments of digital systems in NPPs and yielded satisfactory results [4–7].

In this paper, the ET/FT method was used to perform reliability assessment of one digital four-channel RPS within the design phase; the main contributions for system risk were identified by importance and sensitivity analysis and

two preliminary schemes for the system design optimization were also proposed and quantitatively evaluated.

2. Target System Description

The present paper estimated the reliability of a digital four-channel RPS during the design phase, with the intention of validating if it satisfies the specified reliability goal and obtaining meaningful risk information about the system for design improvement. The reliability goal for the RPS specified by the system requirement specification is as follows:

(i) Probability of failure to generate reactor trip signal should be equal to or less than 10^{-7} per demand.

(ii) Frequency of the generation of the spurious trip signal should be equal to or less than 0.1/year

The schematic diagram of the four-channel RPS is provided in Figure 1. The system includes four channels (i.e., IP, IIP, IIIP, and IVP). Each channel consists of two subchannels (i.e., subchannel-1 and subchannel-2) with functional diversity and eight subchannels constituting subsystem-1 and subsystem-2. Each subchannel (see Figure 2) contains three types of signal condition modules (SCMs), that is, analog signal conditioning modules (ACM), digital signal conditioning modules (DCM), and thermocouple signal conditioning modules (TCM), two types of input modules, that is, analog input modules (AI) and digital input modules (DI), input/output extended modules (EXT), digital output modules (DO), processor modules (CPU), and communication modules (COM). Among them, CPU and COM are hot-standby redundancy configurations. Conditioning modules are used to condition, isolate, and distribute signals from sensors. AI and DI convert the signals into numerical format then transmit them to CPUs through EXT. In a subchannel, the CPU compares the signals with the predefined setpoint value and generate a local coincidence signal (LCS) if the threshold value is reached; with threshold judgment results of other three subchannels transmitted by COM, the CPU performs two-out-of-four voting logic and generation trip signal when there are two or more LCSs. Output signals of subchannel-1 and subchannel-2 of each channel are connected with "OR" gate and then open one pair of reactor trip breakers. If two out of four pairs of reactor trip breakers open, the reactor will be shut down.

For most of the design basis accidents, there are two kinds of diversity of sensor signals used to generate shutdown signals; and signals without diversity are transmitted to two subchannels through SCM.

3. Fault-Tree Analysis

3.1. Model Development. The present paper is focused on the safety function of the RPS to generate a reactor trip signal. Two failure modes of the system are considered, that is, failing to generate reactor trip signal and generating spurious signal.

In order to envelop situations with different acquisition signal quantities and obtain conservative calculation results, Top Events are defined as follows based on the principle for functions allocation of the system:

(i) Failing to generate reactor trip signal on demand under three sensor signals without diversity (RT 3IN FD).

(ii) Generating a spurious trip signal under one sensor signal with diversity (RT 1IN ST).

Since the component configurations for different types of measurement signal to generate trip signal just distinguish on conditioning and input modules, it might as well select analog signal to develop a case model and only simple modifications will be needed for digital or thermocouple signal. The analysis is based on the following assumptions:

(i) The analysis places emphasis on the digital system itself and the failures of sensors, reactor trip breakers, and associated relays with them are not considered.

(ii) Loss of power supply of functional modules would cause their unavailability and such has a negative effect on the implementation of preset safety functions of the system. However, since there is not enough information about the supply power system at the time of the performance of this analysis and it can believe that the complete failure probability of it is very low because the power supply of a cabinet generally has triple redundancy configuration, the modeling of the supply power system exclude in the present paper.

(iii) LCS signals used for voting to generate trip signals are transmitted among channels of the RPS through the data communication network. Such effect of its failure on the reliability of the RPS should not be ignored, which may result from failure of hardware or software of communication module or faults in transmission medium of communication cable and would lead to loss of communication of LCS signals. Nonetheless, there was not enough information about the data communication network when this study was conducted and the reliability analyses of it are excluded.

(iv) The faults in different software modules of the digital system may result in different failures. Although, from the point of view of modeling convenience, software failure can be divided into two categories depending on whether the effect of the failure is failure of a single module or simultaneous failure of multiple modules that is the same as CCF. Examples of the failure categories may be faults in application software and faults in software functional requirements specification. Since debates on the applicability of current quantitative software

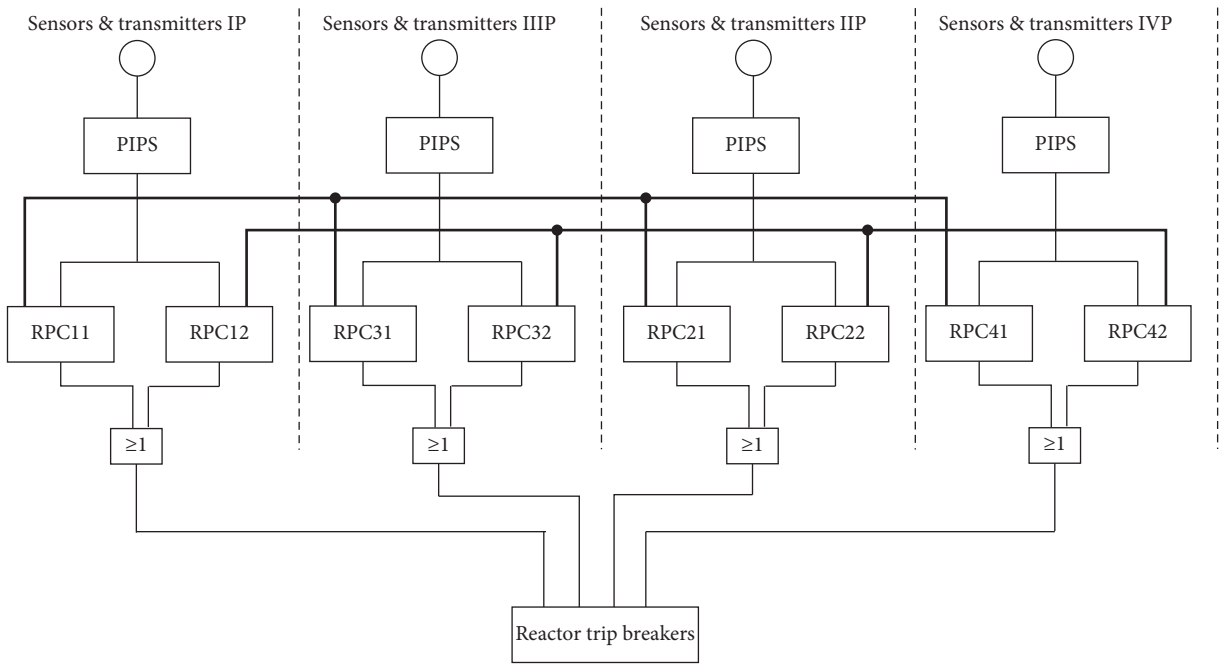

Figure 1: The schematic diagram of the four-channel RPS.

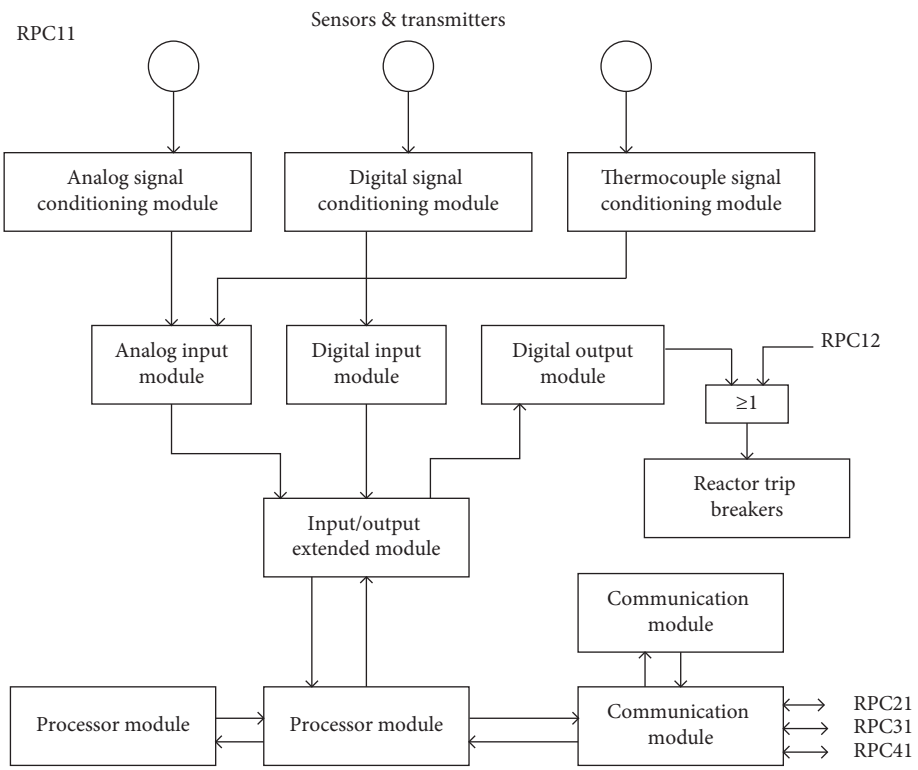

Figure 2: The layout of subchannel-1 of Channel IP.

reliability methods and the lack of data and information of the system software, its modeling was not included in the current study.

(v) It is supposed that the human errors have no effect on the generation of the automatic signal and human reliability analysis is out of scope.

(vi) To be conservative in terms of reliability, it is assumed that once the failure of one module is detected, repair activity occurs and results in the unavailability of the module.

(vii) According to the maintainability and availability requirements of the RPS specified in the system requirement specification, the meantime to repair (MTTR) and periodic test interval (TI) for modules are assumed to be four hours and six months, respectively.

The basic events used in the FT models for the Top Events are defined based on the failures of the modules. Failures of a module are classified according to their detectability and effects on module function, including the following [8]:

(i) Detected failure (D): the failure is detected and the repair leads to the availability of the module.

(ii) Undetected safe failure (US): the failure is undetected and results in an increase in the probability of spurious action.

(iii) Undetected unsafe failure (UU): the failure is undetected and the function of the module is completely lost.

The FT models for a Top Event were constructed based on the following principles:

(i) Find out all failure signal combinations that will result in the Top Event.

(ii) For each signal in a combination, find out all failure modes and input signals combinations of the module that will lead to the signal.

The topic logics of FT models for RT 3IN FD and RT 1IN ST are shown in Figures 3 and 4, respectively.

3.2. Quantitative Analysis. The reliability models used for basic events in the quantitative analysis include a repairable component for detected failure and a periodically tested component for undetected failure. The unavailability $Q(t)$ of the repairable component is modeled by

$$Q(t) = \frac{\lambda}{\lambda + \mu}\left(1 - e^{-(\lambda+\mu)t}\right), \quad (1)$$

where λ and μ (=1/MTTR) are the failure rate and repair rate of the component, respectively. The long-term unavailability of the component is $Q = \lambda/(\lambda + \mu)$. The unavailability $Q(t)$ of periodically tested component is modeled by:

$$Q(t) = 1 - e^{-\lambda\left(t - T_i\right)}, \quad T_i = 0, \mathrm{TI}, 2\mathrm{TI}, \ldots, \quad (2)$$

where λ and TI are failure rate and test interval of the component, respectively. The mean unavailability of the component is $Q = 1 - (1 - e^{-\lambda \mathrm{TI}})/(\lambda \mathrm{TI})$.

The failure data of the modules constituting the system was derived from results of failure modes, effects, and diagnostic analysis (FMEDA) of the modules. Parameters mainly include detected failure rate (λ_{D}), undetected safe failure rate (λ_{US}), and undetected unsafe failure rate (λ_{UU}) of modules, as shown in Table 1.

Two types of CCFs of the modules were considered: (1) CCFs of modules with hot-standby configuration in the same subchannel and (2) CCFs of identical modules of four channels in the same subsystem. They are modeled by Beta model and Multiple Greek Letter model, respectively [9]. The parameters of CCFs models used in this analysis are shown in Table 2.

The parameter uncertainty was considered in the analysis. Since recognized weaknesses in the data, large error factor (EF) was assumed for the parameter, that is, 5 for failure rate and 3 for β, γ, and δ [10]. In addition, the parameter was assumed to be lognormally distributed. The propagate of parameter uncertainties in terms of variation of system failure probability was evaluated.

The calculation results for three types of signals are shown in Tables 3 and 4. The results indicate that when the input scram parameters are thermocouple signals the probability of the RPS failing to generate a trip signal on demand is 1.47×10^{-6} with a 95% upper bound of 4.63×10^{-6} in case of considering CCFs, which is larger than the other two types of signals. If contributions of CCFs are ignored, this value is 2.12×10^{-11} with a 95% upper bound of 3.83×10^{-10}. For the same signal type, the frequency of the system generating spurious trip signal is 7.94×10^{-4}/year with a 95% upper bound of 5.71×10^{-3}/year on condition that the FT model includes CCFs, which is also larger than the other two types of signals. When the CCFs are excluded in the system reliability model, the frequency is 2.70×10^{-5}/year with a 95% upper bound of 1.41×10^{-4}/year. Taking CCFs into account, the system reliability does not fulfill the specified reliability goal (see section 2) with regard to the probability of failure on demand of the system function. The results make it clear that CCFs of modules are the main contributors of the system failure; this is consistent with the consensus that the safety-critical protection system with redundancy multiple-channel is remarkably affected by CCFs [4, 11].

4. Importance and Sensitivity Analysis

From the perspective of safety, the probability of the system failure on demand to generate trip signal is more of a concern in PSA. Such importance and sensitivity analyses were performed to identify the significant factors which contribute to the failure on demand of the RPS (selecting analog signal as case study). The factors include individual basic event (BE), input parameters (e.g., failure rate), and components (modules of the RPS). Importance measures commonly used include Fussell–Vesely (FV), risk decrease factor (RDF), and risk increase factor (RIF). FV of factor i

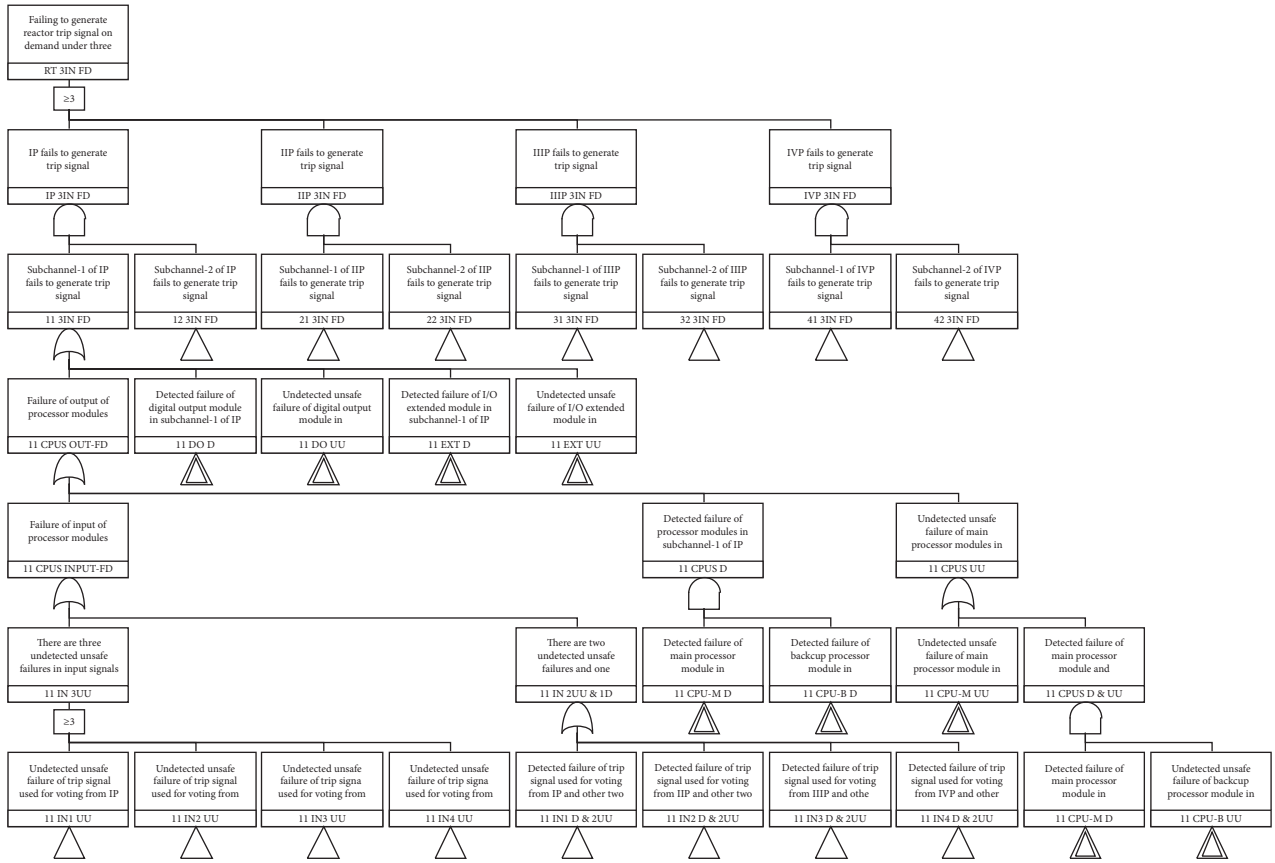

Figure 3: Top logic of FT model for RT 3IN FD.

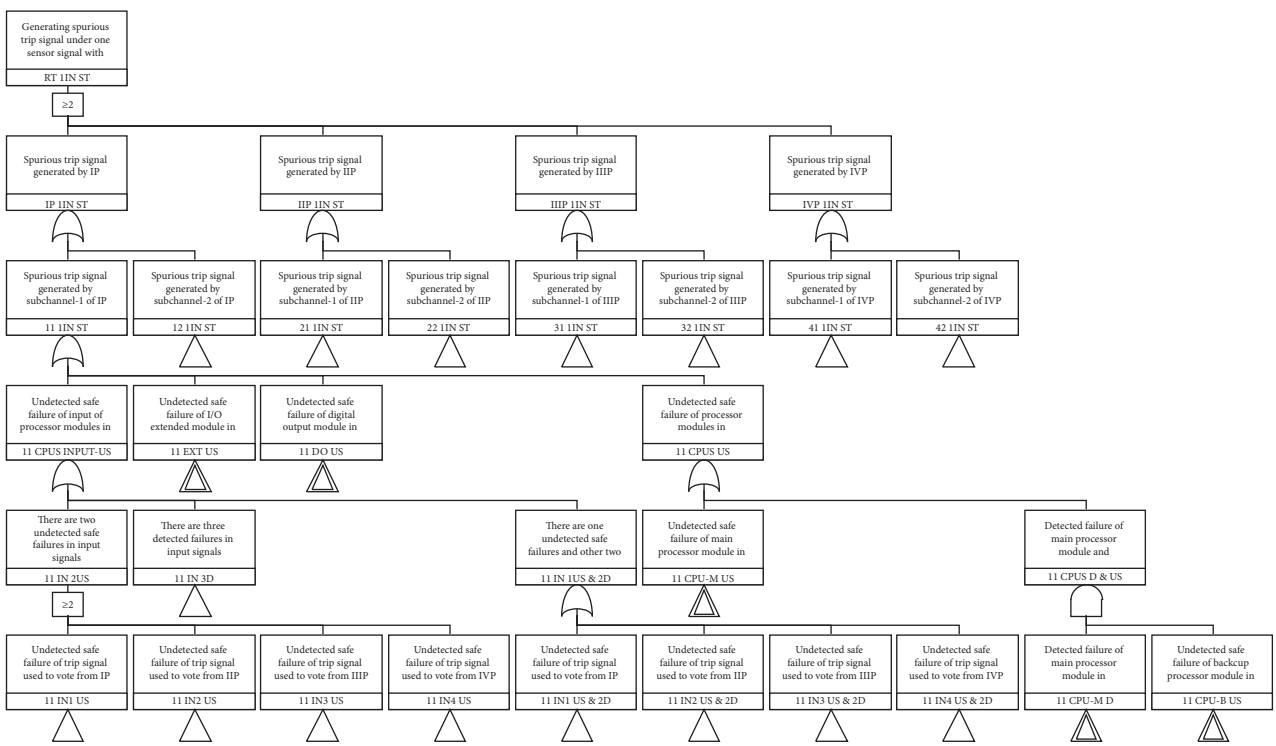

Figure 4: Top logic of FT model for RT 1IN ST.

Table 1: Failure rates of components (/h).

Module	λ_D	λ_{US}	λ_{UU}
ACM	2.52×10^{-6}	7.50×10^{-8}	1.25×10^{-8}
DCM	6.35×10^{-7}	3.02×10^{-9}	3.64×10^{-9}
TCM	4.61×10^{-6}	7.72×10^{-8}	2.05×10^{-8}
AI	2.02×10^{-6}	3.83×10^{-8}	9.95×10^{-9}
DI	9.00×10^{-7}	9.45×10^{-9}	1.71×10^{-9}
EXT	6.75×10^{-7}	5.70×10^{-9}	1.11×10^{-9}
COM	7.65×10^{-7}	6.60×10^{-9}	1.11×10^{-9}
CPU	3.68×10^{-6}	3.90×10^{-8}	1.30×10^{-8}
DO	7.38×10^{-7}	9.46×10^{-8}	1.24×10^{-9}

Table 2: Parameters of CCFs models.

Model	Failure mode	β	γ	δ
Beta	Detected failure	0.005	—	—
	Undetected failure	0.01	—	—
MGL	Detected failure	0.009	0.5	0.33
	Undetected failure	0.018	0.5	0.33

Table 3: Probabilities of the RPS failing to generate a trip signal on demand.

Signal type	CCFs included			CCFs excluded		
	Mean	5^{th} perc.	95^{th} perc.	Mean	5^{th} perc.	95^{th} perc.
Analog	8.94×10^{-7}	3.49×10^{-8}	2.86×10^{-6}	4.54×10^{-12}	1.23×10^{-12}	8.57×10^{-11}
Digital	2.60×10^{-7}	1.02×10^{-8}	7.57×10^{-7}	1.03×10^{-13}	2.91×10^{-14}	1.97×10^{-12}
Thermocouple	1.47×10^{-6}	5.98×10^{-8}	4.63×10^{-6}	2.12×10^{-11}	5.74×10^{-12}	3.83×10^{-10}

Table 4: Calculation results for Top Event RT 1IN ST (1/yr).

Signal type	CCFs included			CCFs excluded		
	Mean	5^{th} perc.	95^{th} perc.	Mean	5^{th} perc.	95^{th} perc.
Analog	5.97×10^{-4}	1.12×10^{-4}	1.88×10^{-3}	1.94×10^{-5}	1.43×10^{-5}	9.47×10^{-5}
Digital	2.51×10^{-4}	4.61×10^{-5}	7.88×10^{-3}	6.11×10^{-6}	3.82×10^{-6}	3.23×10^{-5}
Thermocouple	7.94×10^{-4}	1.47×10^{-4}	2.50×10^{-3}	2.70×10^{-5}	1.99×10^{-5}	1.41×10^{-4}

(related to individual BE or multiple BEs constituting a group) represents the contribution of the factor on the system risk, defined as

$$\mathrm{FV}_i = \frac{Q_{\mathrm{Top},i}}{Q_{\mathrm{Top}}}, \tag{3}$$

where Q_{Top} is the probability of the Top Event. $Q_{\mathrm{Top},i}$ is the probability of the Top Event calculated based only on all minimum cut sets including BEs related to factor i.

RDF of factor i is a measure that indicates the decrease of system risk assuming the nonoccurrence of BEs related to the factor. Mathematically, it is calculated as

$$\mathrm{RDF}_i = \frac{Q_{\mathrm{Top}}}{Q_{\mathrm{Top},p(i)=0}}, \tag{4}$$

where $Q_{\mathrm{Top},p(i)=0}$ is the probability of the Top Event with assuming that probabilities of BEs related to factor i are zero.

RIF is the opposite of RDF, that is, it expresses the increase of system risk based on BEs related to the factor certainly occurring. It is expressed as

$$\mathrm{RIF}_i = \frac{Q_{\mathrm{Top},p(i)=1}}{Q_{\mathrm{Top}}}, \tag{5}$$

where $Q_{\mathrm{Top},p(i)=1}$ is the probability of the Top Event with assuming that probability of BEs related to factor i is one.

The sensitivity of factor i related to individual BE or multiple BEs on the probability Top Event is defined as

$$\mathrm{Sens}_i = \frac{Q_{\mathrm{Top},U}}{Q_{\mathrm{Top},L}}, \tag{6}$$

where $Q_{\mathrm{Top},U}$ and $Q_{\mathrm{Top},L}$ are the probabilities of the Top Event based on probability of BEs related to factor i multiplied by a sensitivity factor (SF) and divided by SF, respectively. When the analysis object is the input parameter,

Table 5: Importance and sensitivity of the selected BEs on system risk.

Number	Basic event	Probability	FV	RDF	RIF	Sens
1	ACM-1 UU-CCF-ALL	8.04×10^{-8}	8.99×10^{-2}	1.10	1.12×10^{6}	1.97
2	ACM-2 UU-CCF-ALL	8.04×10^{-8}	8.99×10^{-2}	1.10	1.12×10^{6}	1.97
3	ACM-3 UU-CCF-ALL	8.04×10^{-8}	8.99×10^{-2}	1.10	1.12×10^{6}	1.97
4	ACM-1 UU-CCF-123	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
5	ACM-1 UU-CCF-124	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
6	ACM-1 UU-CCF-134	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
7	ACM-1 UU-CCF-234	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
8	ACM-2 UU-CCF-123	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
9	ACM-2 UU-CCF-124	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
10	ACM-2 UU-CCF-134	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
11	ACM-2 UU-CCF-234	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
12	ACM-3 UU-CCF-123	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
13	ACM-3 UU-CCF-124	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
14	ACM-3 UU-CCF-134	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
15	ACM-3 UU-CCF-234	5.44×10^{-8}	6.08×10^{-2}	1.06	1.12×10^{6}	1.64
16	1 ACM-1 UU	2.66×10^{-5}	2.27×10^{-5}	1.00	1.85	1.00
17	2 ACM-1 UU	2.66×10^{-5}	2.27×10^{-5}	1.00	1.85	1.00
18	3 ACM-1 UU	2.66×10^{-5}	2.27×10^{-5}	1.00	1.85	1.00
19	4 ACM-1 UU	2.66×10^{-5}	2.27×10^{-5}	1.00	1.85	1.00

Note. ACM-1, 2, 3 represent ACMs for three sensor signals. UU-CCF-ALL represents common cause undetected unsafe failure of four identical modules of all channels. UU-CCF-XYZ (X, Y, $Z = 1, 2, 3, 4$) represents common cause undetected unsafe failure of four identical modules of X, Y, and Z channels, where 1, 2, 3, and 4 represent IP, IIP, IIIP, and IVP respectively. X ($X = 1, 2, 3, 4$) represents channels.

the above two quantities, respectively, represent the probabilities of the Top Event under conditions that the parameter is multiplied and divided by SF. In this analysis, SF is defined as 10.

The importance and sensitivity calculation results for the selected BEs, parameters, and components are shown in Tables 5–7. It is shown that undetected unsafe CCFs of ACMs have significant effects on system reliability. TI and λ_{UU} of the ACM, which determine the probabilities of UU of ACMs, are decisive parameters for the system risk. The results show that ACMs are the critical component of the system.

Schemes for system design optimization shall focus on reducing the unavailability of ACMs caused by CCFs which is determined by TI, λ_{UU} of the ACM, and CCF parameter. From the perspective of feasibility, reduction of TI might be more appropriate. In addition, enhancing the capacity of the ACM defending CCF, such as applying diversity, is also an effective approach.

5. Preliminary Optimization Schemes for the System

According to the insights of importance and sensitivity analyses, two preliminary optimization schemes were explored, regarding increase test frequency and adopting different kinds of diverse SCMs. The quantitative evaluations for the improvements were conducted as well.

The probability of the system failing to generate trip signal on demand was calculated under different shorter TI as follows:

(i) Case 1: TI for modules is reduced to three months.

(ii) Case 2: TI for modules is reduced to one month.

The calculation results are shown in Table 8. It is shown that the probability of system failure on demand decreases significantly when TI reduces. However, the reliability requirement of the system is still not explicitly fulfilled. With consideration of the increased maintenance costs associated with increasing the frequency of the periodic test, this approach is not very promising.

Another potential approach is the use of two kinds of diverse SCMs to improve the capacity of SCMs to defense CCF. It should be recognized that although diverse modules usually achieve the same function through different principles, materials, and so forth, it is inappropriate to assume that diverse modules are completely free of CCF, due to the use of small electronic elements manufactured in a globally standardized environment. More appropriate treatment is to assume that the CCF probability of diverse modules decreases to a certain extent. Calculations for the following three cases were performed:

(i) Case 1: the CCF probability of diverse SCMs decreases by 50%

(ii) Case 2: the CCF probability of diverse SCMs decreases by 75%

(iii) Case 3: the CCF probability of diverse SCMs decreases by 90%

The calculation results are shown in Table 9. It indicates that the use of diverse SCMs would markedly improve system reliability, but even if assuming that the CCF probability is reduced to a level that is almost ideal, the system reliability is still not determinately meeting the target.

The analysis results show that the system reliability requirement cannot be fulfilled only by shortening TI or adopting diverse SCMs. More detailed optimization analysis is needed to determine the final system design optimization

Table 6: Importance and sensitivity of the selected parameters on system risk.

Number	Parameter	Value	FC	RDF	RIF	Sens
1	TI	6 months	1.00	1.57×10^{9}	1.12×10^{6}	1.00×10^{2}
2	λ_{UU} (ACM)	1.25×10^{-8}/h	1.00	6.98×10^{5}	1.12×10^{6}	1.00×10^{2}
3	MTTR	4 h	1.01×10^{-4}	1.00	1.10×10^{2}	1.00
4	λ_{D} (ACM)	2.52×10^{-6}/h	1.01×10^{-4}	1.00	4.42	1.00
5	λ_{UU} (AI)	9.95×10^{-9}/h	1.32×10^{-6}	1.00	9.12×10^{3}	1.00
6	λ_{UU} (CPU)	1.30×10^{-8}/h	7.19×10^{-7}	1.00	1.01×10^{3}	1.00
7	λ_{UU} (DO)	1.24×10^{-9}/h	7.25×10^{-8}	1.00	8.24×10^{1}	1.00
8	λ_{UU} (COM)	1.11×10^{-9}/h	7.00×10^{-8}	1.00	1.43×10^{2}	1.00
9	λ_{UU} (EXT)	1.11×10^{-9}/h	7.00×10^{-8}	1.00	1.43×10^{2}	1.00
10	λ_{D} (EXT)	6.75×10^{-7}/h	4.07×10^{-8}	1.00	2.73×10^{1}	1.00

Table 7: Importance and sensitivity of the selected components on system risk.

Number	Component	FC	RDF	RIF	Sens
1	1 ACM-1	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
2	1 ACM-2	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
3	1 ACM-3	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
4	2 ACM-1	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
5	2 ACM-2	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
6	2 ACM-3	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
7	3 ACM-1	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
8	3 ACM-2	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
9	3 ACM-3	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
10	4 ACM-1	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
11	4 ACM-2	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
12	4 ACM-3	2.72×10^{-1}	1.37	1.12×10^{6}	4.57
13	11 CPU-A	3.27×10^{-7}	1.00	6.07	1.00
14	21 CPU-A	3.27×10^{-7}	1.00	6.07	1.00
15	31 CPU-A	3.27×10^{-7}	1.00	6.07	1.00
16	41 CPU-A	3.27×10^{-7}	1.00	6.07	1.00

Note. X ($X = 1, 2, 3, 4$) represents channels. XY ($X = 1, 2, 3, 4$; $Y = 1, 2$) represents subchannels. ACM-1, 2, 3 represent ACMs for three sensor signals; CPU-A represents the main CPU in the subchannel.

Table 8: Probability of the system failure on demand under different TI.

Case	Base case	Case 1	Case 2
TI	6 months	3 months	1 month
Probability of system failure	1.47×10^{-6}	7.33×10^{-7}	2.44×10^{-7}

Table 9: Probability of the system failure on demand with the use of diversity SCMs.

Case	Base case	Case 1	Case 2	Case 3
CCF probability reduction	0%	50%	75%	90%
Probability of system failure	1.47×10^{-6}	7.35×10^{-7}	3.68×10^{-7}	1.47×10^{-7}

scheme, for example, the combination of the above scheme or change of system architecture.

6. Conclusions

In this paper, a safety-related digital four-channel RPS within design phase was assessed by ET/FT method to verify if the system reliability meets specified requirements regarding the function to generate reactor trip signal and to obtain important risk information for design feedback.

The results of the quantitative analysis indicate that the probability of failure on demand of the system to generate trip signal is 1.47×10^{-6} with a 95% upper bound of 4.63×10^{-6} and the frequency of the system generating spurious signal is 7.94×10^{-4}/year with a 95% upper bound of 2.50×10^{-3}. The reliability of the system function regarding generating trip signal on demand does not fulfill the reliability target of the system, that is, below 10^{-7}.

The importance and sensitivity analyses were performed to identify critical factors which have significant impacts on

system reliability and to determine improvement direction. It is found that undetected unsafe CCFs of SCMs dominate the probability of the system failure on demand and TI and λ of the SCMs have very high sensitivity.

Quantitive evaluation for two preliminary optimization schemes relative to the improvement of TI frequency and the use of diverse SCMs was conducted. The analysis results show that neither of them could determinedly improve the system reliability to target level. In the future, more detailed optimization analysis will be performed to determine feasible system design optimization scheme, for example, the combination of the above scheme or change of system architecture.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The author would like to thank the Science and Technology on Reactor System Design Technology Laboratory of Nuclear Power Institute of China for financial support of this work.

References

[1] K. Korsah, R. Wetherington, R. Wood et al., *Emerging Technologies in Instrumentation and Controls: An Update*, Nuclear Regulatory Commission, Washington, DC, USA, NUREG/CR-6888 ORNL/TM-2005/75, 2006.

[2] T. Aldemir, D. W. Miller, M. P. Stovsky et al., *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments*, Nuclear Regulatory Commission, Washington, DC, USA, NUREG/CR-6901, 2006.

[3] T. Aldemir, M. P. Stovsky, J. Kirschenbaum et al., *Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments*, Nuclear Regulatory Commission, Washington, DC, USA, NUREG/CR-6942, 2007.

[4] H. G. Kang and S.-C. Jang, "A quantitative study on risk issues in safety feature control system design in digitalized nuclear power plant," *Journal of Nuclear Science and Technology*, vol. 45, no. 8, pp. 850–858, 2008.

[5] S. J. Lee, W. Jung, and J. E. Yang, "PSA model with consideration of the effect of fault-tolerant techniques in digital I&C systems," *Annals of Nuclear Energy*, vol. 87, no. Part 2, pp. 375–384, 2008.

[6] S. H. Lee, K. S. Son, W. Jung, and H. G. Kang, "Risk assessment of safety data link and network communication in digital safety feature control system of nuclear power plant," *Annals of Nuclear Energy*, vol. 108, pp. 394–405, 2017.

[7] J. H. Bickel, "Risk implications of digital reactor protection system operating experience," *Reliability Engineering & System Safety*, vol. 93, no. 1, pp. 107–124, 2008.

[8] M. Jockenhövel-Barttfeld, S. Karg, C. Hessler et al., "Reliability analyses of digital I&C systems within the verification and validation process," in *Proceedings of the 14th International Probabilistic Safety Assessment & Management Conference (PSAM 14)*, Los Angeles, CA, USA, September 2018.

[9] A. Mosleh, D. M. Rasmuson, and F. M. Marshall, *Guidelines in Modeling Common Cause Failure in Probabilistic Risk Assessment*, Nuclear Regulatory Commission, Washington, DC, USA, NUREG/CR-5485 NEELIEXT-97-01327, 1998.

[10] T. L. Chu, M. Yue, G. Martinez et al., *Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods*, Nuclear Regulatory Commission, Washington, DC, USA, NUREG/CR-6997 BNL-NUREG-90315-2009, 2009.

[11] H. G. Kang and T. Sung, "An analysis of safety-critical digital systems for risk-informed design," *Reliability Engineering & System Safety*, vol. 78, no. 3, pp. 307–314, 2002.